AFFIDAVIT

I, Stephanie Loycano, being duly sworn, declare and state as follows:

I. INTRODUCTION

1. I am a Special Agent for the Federal Bureau of Investigation (herein referred to as the "FBI"). I have been so employed since March of 2020 and attended a 20-week training at the FBI Academy located in Quantico, Virginia. While at the academy, I studied a wide range of subjects to include the fundamentals of law, ethics, behavioral science, interviewing, and report writing, basic and advanced investigative and intelligence techniques, interrogation, and forensic science. I learned how to manage and run counterterrorism, counterintelligence, weapons of mass destructions, cyber and criminal investigations. From the academy, I was assigned to the Pittsburgh Division and placed in the Clarksburg, West Virginia Resident Agency. I have experience investigating various violations in the Northern District of West Virginia to include public corruption, civil rights, fraud, counterterrorism, domestic terrorism, and violent crimes.

II. PURPOSE OF THE AFFIDAVIT

2. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property, and extraction of electronically stored information described in

Attachment B, related to one computer tower: (1) Hewlett-Packard Computer, more fully described in Attachment A (the "TARGET DEVICE"). This item is currently being stored by the FBI, at the Clarksburg West Virginia Resident Agency.

3. As described more fully below, I respectfully submit there is probable cause to believe that the information located on this device constitutes evidence, contraband, fruits, or instrumentalities of criminal violations of 18 U.S.C. § 666 (State or Local Program Fraud, Theft or Bribery Concerning Programs Receiving Federal Funds), 641 (Embezzlement of Public Money, Property, or Records), 654 (Conversion of Property by a Federal Officer or Employee) 1519 (Destruction, Alteration, or Falsification of Records) and 1957 (Money Laundering) (collectively, the "Subject Offenses").

4. The facts set forth in this affidavit are based upon my personal observations, my training and experience, and information obtained from other law enforcement officers and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not purport to set forth all my knowledge of or investigation into this matter. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only with original typographical errors and all dates are approximate.

III. PROPERTY TO BE SEARCHED AND ITEMS TO BE SEIZED

5. The property to be searched is described in Attachment A and the items to be searched are described in Attachment B, both are incorporated herein full by reference.

IV. FACTS AND CIRCUMSTANCES ESTABLISHING PROBABLE CAUSE

6. Based on my training and experience, my personal investigation into this matter, my conversations with law enforcement officers, and my review of law enforcement reports, I know the following:

A. On or about January 27, 2022 Wheeling Police Department Sergeant David Drahos admitted to stealing approximately $70,000 from the Ohio Valley Drug Task Force

7. On or about February 4, 2022 the United Sates Attorney's Office (USAO) of the Northern District of West Virginia along with the Clarksburg Resident Agent in Charge (RAC) of the Drug Enforcement Agency (DEA), provided information to the FBI that on or about January 27, 2022 Sergeant David Drahos (hereinafter referred to as Drahos) of the Wheeling Police Department (WPD) and Commander of the Ohio Valley Drug Task Force (OVDTF) admitted to the Chief of WPD to stealing approximately $70,000 from the OVDTF.

8. Based on my discussion with the WPD Chief of Police, as the Commander of the OVDTF, Drahos was in charge of providing financial information to the Finance Director at WPD. As the Financial Director was not receiving timely documentation from Drahos pertaining to the finances, an impromptu audit was conducted at the OVDTF.

9. Drahos was called in to the Chief's Office and Drahos told the Chief that he took money out of the OVDTF safe to use it for a particular task. Based on information provided by Drahos, Drahos put the money in a box, left the money in the box to go assist the OVDTF with a drug buy and somehow the box was inadvertently thrown out. There was approximately $70,000 missing.

10. The OVDTF is funded by the Appalachia High Intensity Drug Trafficking Areas (HIDTA). HIDTA was created by Congress with the Anti-Drug Abuse Act of 1988, and aids federal, state, local, and tribal law enforcement agencies operating in areas determined to be critical drug-trafficking regions of the United States.

B. Drahos had access to specific Wesbanco bank accounts that were used by the OVDTF

11. Based on my discussion with the WPD Finance Director, there are four individual OVDTF accounts. There is the OVDTF operating account, the state forfeiture account, and two federal forfeiture accounts. There is no debit card associated with the federal accounts, so to take money out of the accounts an individual needs to go to the bank.

12. Drahos was one of two signers on the accounts but only one signer was needed.

13. Based on my discussion with other law enforcement personnel at the OVDTF, Drahos was the main individual who put money in and took money out of the bank accounts. The

other individual was more of a back-up in case Drahos was not available.

14. The Finance Director has access to the online statements and would us the Sage Account, an accounting platform, to reconcile the funds from the OVDTF.

15. Drahos would send monthly overtime and drug money reports/Confidential Informant (CI) reports to the Financial Director. The reports would include the amount of money submitted to HIDTA by the OVDTF for reimbursement. The reimbursement funds would be transferred from HIDTA to the general fund checking account. This fund is where the monies would be kept. When the Financial Director would receive the funds from HIDTA for the drug buy and CI money, he would then transfer the proper amount to the operating fund.

C. Discrepancies between monetary amounts reported to the Financial Director and the monetary amount reimbursed by HIDTA

16. According to the Financial Director, there were a handful of times that the amounts provided to him by Drahos did not match with the reimbursement amounts received from HIDTA.

17. HIDTA would receive reports from Drahos as to what reimbursement amounts were needed and Drahos would provide those figures to the Financial Director.

18. When the Financial Director inquired with HIDTA as to why HIDTA overpaid reimbursements, according to the Financial Director's records, HIDTA advised they paid the amount they were billed.

19. The figure billed to HIDTA would have come from Drahos. Drahos was providing HIDTA with a different figure for reimbursement than what he was providing to the Financial Director.

D. Depletion of accounts and lack of timely documentation by Drahos

20. According to the Financial Director, for the past year (2021), Drahos has not been providing timely reports pertaining to the allocation of funds and the accounts Drahos had access to were depleting.

21. For the past year (2021), the Financial Director would see a routine cashing of $2,000 checks but would not receive the appropriate paperwork pertaining to the use of the monies.

22. For approximately the past year (2021), the Financial Director was not receiving reporting from Drahos. This is when the Financial Director noticed that the operating and federal forfeiture account had been dwindling with no paperwork provided by Drahos to explain the activity.

E. Procedure for documentation of monies spent by the OVDTF

23. All funds going out of the task force had to be documented. As the commander of the task force, Drahos was responsible for tracking these voucher's and making sure they were accurate and appropriately filed.

24. When task force funds were used to make a payment for evidence buys, i.e., drug buys, or payments to C.I.'s a corresponding voucher was completed and filed. These vouchers

were necessary to keep track of the monies. Drahos was then able to appropriately request reimbursement from HIDTA based on the monies that had been used for evidence buys and C.I. payments.

25. Part of Drahos' duties as the Commander of the OVDTF was to provide the Financial Director with monthly Register Reports, which documented the amount of money used during that month and what the money was used for.

Comparison of Register Reports and voucher documentation

26. Subpoena returns received by the WPD included monthly Register Reports submitted by Drahos to the Financial Director for the time frame of December of 2016 through December of 2021.

27. The interim Commander of the OVDTF provided investigators with all vouchers they had on file for the timeframe of December of 2016 through December of 2021.

28. Investigators then compared the monthly Register Reports to the vouchers. Investigators noticed a multitude of discrepancies as well as vouchers that could not be accounted for. Examples of this are as follows:

a. 3/13/2019 - case number 19-0000036 payment for $400.00 - Investigators found that the voucher submitted was for a case payment of $200.00. The register report shows a case payment of $400.00.

b. 4/16/2019 - case number 19-0000077 payment for $220.00 - Investigators found that the voucher

submitted was for a case payment of $120.00. The register report shows a case payment of $220.00.

c. 8/6/2019 - informant payment D19-07 for $60.00 - investigators were unable to find the voucher correlating to this line item Drahos put on his Register Report.

d. 8/6/2019 - informant payment D19-07 for $60.00 - investigators were unable to find the voucher correlating to this line item Drahos put on his Register Report.

e. 1/24/2020 - informant payment D15-12 for $40.00 - investigators were unable to find the voucher correlating to this line item Drahos put on his Register Report.

f. 3/14/2020 - case number 20-000062 payment for $100.00 - investigators were unable to find the voucher correlating to this line item Drahos put on his Register Report.

g. 5/14/2021 - case number 21-00033 payment for $4,000.00 - investigators were unable to find the voucher correlating to this line item Drahos put on his Register Report.

h. 6/16/2021 - case number 21-00054 payment for $3,500.00 - investigators were unable to find the voucher correlating to this line item Drahos put on his Register Report.

i. 12/9/2021 - case number 21-0000099 payment for $3,600.00 - investigators were unable to find the voucher correlating to this line item Drahos put on his Register Report.

Identification of funds that were allegedly paid by OVDTF but were actually paid by another department.

29. The interim Commander and other OVDTF members alerted investigators of two specific payments that were recorded as having been paid by the OVDTF when they were actually paid by the Columbus Police Department.

30. After Drahos' resignation, an excel spreadsheet was located by OVDTF members on Drahos' desk. The spreadsheet documented drug buys that were made in Columbus, Ohio and one of the OVDTF member's names was listed with the withdrawal amount. That OVDTF member had been working with a Detective from the Gang Unit in Columbus and the OVDTF was helping support the operation.

31. The OVDTF member who was assisting Columbus with the operation told investigators that the OVDTF did not use their buy money for these buys and that the buy money used for the operation came from Columbus. The spreadsheet filled out by Drahos made it appear that the money came from the OVDTF. It was confirmed by the OVDTF interim Commander that the two falsified payments were as follows:

a. 5/14/2021 - case number 21-00033 payment for $4,000.00 - investigators were unable to find the

voucher correlating to this line item Drahos put on his Register Report.

b. 6/16/2021 – case number 21-00054 payment for $3,500.00 – investigators were unable to find the voucher correlating to this line item Drahos put on his Register Report.

i. This falsification by Drahos was verified through the subpoena return we received from WPD, which provided the monthly Register Report showing Drahos claiming the OVDTF made these drugs purchases.

F. Evidence of the commission of the crimes under investigation is likely to be found on the TARGET DEVICE.

32. Based on investigator's discussions with other OVDTF members and a review of the WPD subpoena return information pertaining to the monthly Register Reports, reports which were completed by Drahos through accounting software that Drahos had access to through the use of his work computer(s) at the OVDTF, investigators believe additional evidence of the commission of the crimes under investigation could be located on the Target Device.

33. Based on the facts set forth above, I submit that there is probable cause to believe that the crimes of State or Local Program Fraud, Theft or Bribery Concerning Programs Receiving Federal Funds, Embezzlement of Public Money, Property, or Records, Conversion of Property by a Federal Officer or Employee, Destruction, Alteration, or

Falsification of Records Money Laundering committed at the OVDTF by Drahos and that information found on the TARGET DEVICE, retrieved from the OVDTF, will provide evidence, contraband, fruits, and instrumentalities of these crimes.

V. ELECTRONIC STORAGE AND FORENSIC ANALYSIS

1. Based on my knowledge, training, and experience, I know that electronic devices, such as the TARGET DEVICE, can store information for long periods of time. Similarly, things that have been viewed via the internet are typically stored for a period of time on the device. This information can sometimes be recovered with forensic tools.

2. Searching for the evidence described in Attachment B may require a range of data analysis techniques. In some cases, agents and computer analysts may be able to conduct carefully targeted searches that can locate evidence without requiring a time-consuming manual search through unrelated materials that may be commingled with criminal evidence. In other cases, however, such technique may not yield the evidence described in the warrant. Criminals can mislabel or hide information, encode communications to avoid using key words, attempt to delete information to evade detection, or take other steps designed to frustrate law enforcement searches for information. These steps may require agents and law enforcement or other analysts with appropriate expertise to conduct more extensive searches, such as scanning storage areas unrelated to things described in Attachment A or perusing all stored information briefly to determine whether it falls within the scope of the warrant. In

light of these difficulties, FBI intends to use whatever data analysis techniques appear necessary to locate and retrieve the evidence described in Attachment B.

3. There is probable cause to believe that things that were once stored on the computer may still be stored there, for at least the following reasons:

1. Based on my knowledge, training, and experience, I know that files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on an electronic device, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

2. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space-that is, in space on the storage medium that is not currently being used by an active file-for longs periods of time before they are overwritten. In addition, a device's operative system may also keep a record of deleted data in a "swap" or "recovery" file.

3. Wholly apart from user-generated files, storage media-in particular, electronic devices' internal hard drives-contain electronic evidence of how a device has been used, what it has been used for, and who has used it. For examples, this

forensic evidence can take the form of operating system configurations, artifacts from operating systems or application operation; file system data structures, and virtual memory "swap" or paging files. Device users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

4. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache".

4. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described in the warrant, but also forensic evidence that establishes how the device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the device because:

1. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file.

2. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

3. A person with appropriate familiarity with how an electronic device works may, after examining the forensic

evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them and when.

4. The process of identifying the exact electronically stored information on storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

5. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, is necessary to establish that a particular thing is not present on a storage medium.

5. *Nature of examination*. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant your affiant is applying for would permit the examination of the Target Device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium. This may expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

6. *Manner of execution*. Because this warrant seeks only permission to examine a device already in law enforcement's

possession, the execution of this warrant does not involve the physical intrusion onto a premise. Consequently, I submit there is probable cause for the Court to authorize execution of the warrant at any time in the day or night.

VI. JURISDICTION

34. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is "a district court of the United States… that – has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

VII. CONCLUSION

35. Based on the foregoing, I request that the Court issue the requested warrant.

STEPHANIE LOYCANO, Special Agent
Federal Bureau of Investigation

Subscribed to and sworn
before me on June 2, 2022

THE HONORABLE MICHAEL J. ALOI
UNITED STATES MAGISTRATE JUDGE